REMARKS/ARGUMENTS

This amendment is responsive to the Final Office Action mailed June 23, 2008. Prior to this amendment, claims 1-8 and 10-34 were pending. In this amendment, claims 1, 19, 28, and 32 are amended, claims 20 and 30 are canceled and claims 35-36 are added. No new matter is added. Thus, after entry of this amendment, claims 1-8, 10-19, 21-29, and 31-36 are pending.

Claim Rejections - 35 USC § 102(b), Hodgson

Claims 1-8, 10-17, 19-20, and 22-32 are rejected as being anticipated by Hodgson et al. (U.S. Patent Pub. No. 2002/0123972)("*Hodgson*"). The Office Action alleges that *Hodgson* teaches each and every limitation in these claims. This rejection is traversed.

Anticipation has not been established because each and every limitation is not taught by *Hodgson*. "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). MPEP 2131.

Claim 1

Each and every limitation of claim 1 as amended is not disclosed by *Hodgson*. Support for the amendments can be found throughout the specification, including such places as Fig. 1 and P[0039], P[0041], and p[0053]. For example, claim 1 recites in part:

> an Access Control Server (ACS) configured to receive a request for passcode authentication of a Primary Account Number (PAN) <u>from a merchant server,</u> and configured to request a passcode corresponding to the PAN <u>from a cardholder device, wherein the ACS is associated with an issuer of the PAN</u>

(*emphasis added*). The Office Action appears to equate the ACS with the consumer computer (*Hodgson* Fig. 2, 14). The Office Action cites p[0090] and Figure 2A, step 210 of *Hodgson* as disclosing the ACS. (Office Action Pg. 4). The portions of the reference cited describe a user using a consumer computer to make a purchase, receiving a request from the merchant web site to request passcode authentication, and receiving the PIN by the consumer's computer. (*Hodgson* P[0090], Fig. 2A). This does not disclose *wherein the ACS is associated with an issuer of the PAN* because the consumer computer is not associated with an issuer. Furthermore, neither the merchant using the STMS merchant framework or the STMS itself are associated with an issuer of the PAN. Even if those elements are considered to be the ACS, they still are not associated with an issuer. As such, *Hodgson* does not disclose *wherein the ACS is associated with an issuer of the PAN.* Withdrawal of the rejection of claim 1 and the claims which depend therefrom is respectfully requested.

Claim 16

Each and every limitation of claim 16 is not disclosed by *Hodgson*. For example, claim 16 recites in part:

> **a front end Hardware Security Module (HSM) coupled to the ACS, and configured to generate the hash value based in part on the unique transaction identifier**, and further configured to receive an encrypted PIN, decrypt the PIN to recover a clear form of the PIN, and generate a local encrypted PIN using a local encryption key

(*emphasis added*). The Office Action alleges this is disclosed in *Hodgson* P[0027] and P[0154]. (Office Action Pg. 8). *Hodgson* describes generically the ability of a HSM to encrypt and decrypt data using various encryption algorithms, such as triple DES. (*Hodgson* P[0027], P[0154]). This does not disclose *a front end Hardware Security Module (HSM) coupled to the ACS, and configured to generate the hash value based in part on the unique transaction identifier.*

First, encryption/decryption and a hash value are not equivalent. Encryption/Decryption is used to maintain data secrecy, whereas a hash function is used to maintain data integrity (e.g. ensuring data has not been altered). Even if for the sake of argument a hash value is considered equivalent to encryption/decryption, *Hodgson* still does not disclose encryption/decryption based on a unique transaction identifier.

Second, *Hodgson* does describe the use of a hash value based on a unique transaction identifier. (*Hodgson* P[0090]). However, the hash value as described in *Hodgson* is generated in the STMS-MF (Id.) This does not disclose *a front end Hardware Security Module (HSM) coupled to the ACS, and configured to generate the hash value based in part on the unique transaction identifier*, because the STMS-MF is not a hardware security module. As such, withdrawal of the rejection of claim 16, and the claims which depend therefrom is respectfully requested.

Claim 18

Each and every limitation of claim 18 is not disclosed by *Hodgson*. For example, claim 18 recites in part:

> an Access Control Server (ACS) configured to receive a request for Personal Identification Number (PIN) authentication of a Primary Account Number (PAN), and configured to generate a request for a PIN corresponding to the PAN, **the request for the PIN including an instruction to provide the PIN to a destination address**; and
>
> **a front end Hardware Security Module (HSM) having said destination address** and coupled to the ACS, and configured to receive an encrypted PIN, decrypt the PIN to recover a clear form of the PIN, and generate an Acquirer Working Key (AWK) encrypted PIN using an AWK encryption key, and configured to communicate the AWK encrypted PIN to an authentication network.

(*emphasis added).* The Office Action alleges *the request for the PIN including an instruction to provide the PIN to a destination address*, is disclosed in *Hodgson* P[0087]. (Office Action Pg. 9). *Hodgson* describes an e-mail being sent to the e-mail address used to register the PinPad as a confirmation of the transaction. (*Hodgson* P[0087]). This does not disclose *the request for the PIN including an instruction to provide the PIN to a destination address,* because the PIN is not provided in the e-mail sent as a confirmation. Sending the PIN in an e-mail would further render *Hodgson* unsuitable for the intended purpose, as including a PIN in an e-mail would expose the PIN in an insecure e-mail environment.

Furthermore, *Hodgson* does not disclose *a front end Hardware Security Module (HSM) having said destination address*. The Office Action alleges that a destination address is the e-mail address used to register the PinPad, as discussed above. *Hodgson* does not disclose the PinPad itself having an e-mail address. As such, *Hodgson* does not disclose *a front end Hardware Security Module (HSM) having said destination address.* As such, withdrawal of the rejection of claim 18 is respectfully requested.

Claim 19

Each and every limitation of claim 19 as amended is not disclosed by *Hodgson.* Claim 19 has been amended to incorporate the limitations present in claim 20. For example, claim 19 as amended recites in part:

> requesting a Personal Identification Number (PIN) corresponding to a Primary Account Number (PAN) wherein requesting the PIN includes generating a unique transaction identifier, generating a hash value with a front end Hardware Security Module (HSM) based in part on the unique transaction identifier, generating a query having the unique transaction identifier and hash value as fields in the query, and communicating the query

(*emphasis added). Hodgson* does not disclose *generating a hash value with a front end Hardware Security Module (HSM) based in part on the unique transaction identifier.* This limitation is similar to the limitation present in claim 16, and the arguments presented with respect to claim 16 apply to claim 19. As such, withdrawal of the rejection of claim 19, and the claims which depend therefrom, is respectfully requested.

Claim 28

Each and every limitation of claim 28 as amended is not disclosed by *Hodgson.* Claim 28 has been amended to incorporate the limitations present in claim 30. For example, claim 28 as amended recites in part:

> **receiving an encrypted Personal Identification Number** (PIN) corresponding to a Primary Account Number (PAN) **in a front end Hardware Security Module** (HSM) over a Secured Sockets Layer (SSL) internet connection between a cardholder device and the front end HSM, wherein **the PIN is exclusively SSL encrypted;**

(*emphasis added). Hodgson* does not disclose receiving an encrypted PIN in a front end HSM wherein the PIN is exclusively SSL encrypted. *Hodgson* does describe SSL encryption, however it describes SSL encryption of the PIN as an additional encryption, not an exclusive encryption. *Hodgson* states:

> At arrow 3), software causes the browser to **further encrypt** the message with 128bit SSL and **transmit it directly to STMS** 30 (see FIG. 9).

(*Hodgson,* P[0076],*emphasis added).* As such, *Hodgson* does not disclose *the PIN is exclusively SSL encrypted*. Furthermore, *Hodgson* states the encrypted PIN is transmitted directly to the STMS. The STMS is not a hardware security module. As such, *Hodgson* does not disclose receiving an encrypted PIN over a SSL connection *in a front end hardware security module.* Withdrawal of the rejection of claim 28, and the claims that depend therefrom, is respectfully requested.

Claim 32

Each and every limitation of claim 32 as amended is not disclosed by *Hodgson.* Support for the amendment of claim 32 can be found throughout the specification, including such places as P[0085]. For example, claim 32 recites in part:

> querying a cardholder for a Personal Identification Number (PIN) corresponding to a Primary Account Number (PAN);
> receiving in a front end Hardware Security Module (HSM) an encrypted PIN and at least a portion of the encryption data from the cardholder in response to the query

(*emphasis added*). *Hodgson* does not disclose receiving an encrypted PIN from a cardholder in a front end hardware security module in response to a query for the PIN. *Hodgson* describes sending an HTML page to a consumer's computer to request a payment. (*Hodgson* P[0068]). *Hodgson* further describes the HTML page instructing the consumer to swipe their credit card into a PinPad, and enter a PIN. (*Hodgson* P[0073]). This is the only place in *Hodgson* where a consumer enters his PIN, and when he enters it into the PinPad, he is not entering the PIN in an encrypted format. As such, if the PinPad is considered the front end HSM, it does not receive an encrypted PIN *from the cardholder.* Furthermore, any of the other HSMs described in *Hodgson* do not receive input from the consumer, but rather receive input from the STMS or a Payment Processor. (*Hodgson,* Fig. 1A). As such, withdrawal of the rejection of claim 32 is respectfully requested.

New Claims

Claims 35 and 36 are added. Support for the newly added claims can be found throughout the specification including such places as P[0082] and Fig. 7. Claims 35 and 36 are patentable over the cited reference because the cited reference does not disclose encryption data comprising a transaction ID, a base redirection url, and a http redirect type. The cited reference also does not disclose a hashed message authentication code based on the transaction ID, the base redirection url, and the http redirect type.

CONCLUSION

In view of the foregoing, Applicants believe all claims now pending in this Application are in condition for allowance and an action to that end is respectfully requested.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 415-576-0200.

Respectfully submitted,

/Preetam B. Pagar/

Preetam B. Pagar
Reg. No. 57,684

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 415-576-0200
Fax: 415-576-0300
PBP:scz
61424094 v1